IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

SOUTHWEST AIRLINES CO.,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**Case No. 3:21-cv-00098-E**
	§	
KIWI.COM, INC. and KIWI.COM S.R.O.,	§	
	§	
Defendants.	§	

PLAINTIFF'S RESPONSE TO DEFENDANTS' MOTION TO DISMISS CFAA CLAIM

Michael C. Wilson
Texas State Bar No. 21704590
mwilson@munckwilson.com
S. Wallace Dunwoody
Texas Bar. No. 24040838
wdunwoody@munckwilson.com
Amanda K. Greenspon
Florida Bar No. 1014584
agreenspon@munckwilson.com
Julie M. Christensen
Texas State Bar No. 24105601
jchristensen@munckwilson.com
MUNCK WILSON MANDALA, LLP
12770 Coit Road, Suite 600
Dallas, Texas 75251
Telephone: (972) 628-3600

COUNSEL FOR PLAINTIFF
SOUTHWEST AIRLINES CO.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

I. INTRODUCTION

In seeking dismissal of Southwest's CFAA claims, Kiwi's motion ignores the First Amended Complaint's ("Complaint") extensive allegations that Kiwi is "accessing Southwest's computer systems … ***without authorization***, bypassing Southwest's security systems intended to block automated traffic and bots from using Southwest's website, and hacking the Southwest application program interface ("API")."[1] While Kiwi touts *Van Buren v. United States*, 141 S. Ct. 1648 (2021) as controlling here, *Van Buren* focused on a single term in CFAA (the "exceeds authorized access"); it did not analyze the scope of the "without authorization" clause of the CFAA.[2] Here, Kiwi's motion does not controvert the Complaint's description of how Kiwi is hacking and circumventing security measures Southwest has implemented to block Kiwi's access to Southwest's computer system.[3] Nor does Kiwi respond to the allegations that, most recently, Kiwi's hacking involves accessing Southwest's API, a part of Southwest's computer system that requires an API key and sits behind a firewall.[4] These facts plead a CFAA violation based on unauthorized access in a "gates down" environment, as endorsed by *Van Buren.*

Moreover, *Van Buren* expressly left open whether non-technological methods such as contract terms or cease-and-desist letters support a CFAA claim for unauthorized access.[5] Southwest's Complaint alleges (and Kiwi does not refute) that Southwest's Website Terms and Conditions expressly prohibit *any* web scraping programs or bots to access flight and fare data, as

---

[1] D.I. 53, First Amended Complaint, at ¶ 16.
[2] *See U.S. v. Eddings*, No. 5:19-cr-00535, 2021 WL 2527966, at *4 (E.D. Pa. June 21, 2021). *Van Buren* involved only the "exceeds authorized access" prong of § 1030(a)(2) and there was no dispute that the defendant had "access[ed] a computer with authorization." 141 S. Ct. at 1654.
[3] D.I. 53, First Amended Complaint, at ¶¶ 75-81.
[4] *See* D.I. 41, Declaration of Michael Erdman, at ¶ 12.
[5] *Van Buren*, 141 S. Ct. at 1659 n.8 ("For present purposes, we need not address whether this inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies.").

well as prohibit conduct that "circumvent[s] any measure implemented by Southwest aimed at preventing violation of the Terms [and Conditions]."[6] Southwest also repeatedly has informed Kiwi in cease and desist letters that it is not authorized to scrape Southwest's proprietary information.[7] In short, Southwest properly has pleaded that Kiwi is hacking and accessing Southwest's computer systems "without authorization" over Southwest's express written objections and best efforts to stop it.

Finally, the nature and extent of Kiwi's unauthorized access are factual questions that cannot be resolved under Rule 12, and Kiwi does not challenge these allegations; thus, the Court must accept them as true for purposes of this motion. Southwest has properly pleaded its claims under the CFAA. Kiwi's motion should be denied.

II. UNCONTESTED COMPLAINT ALLEGATIONS

The allegations in the Complaint, except insofar as controverted by opposing affidavits, must be taken as true, and all conflicts in the facts must be resolved in favor of the plaintiff.[8] Kiwi does not controvert any of the following allegations from Southwest's Complaint:[9]

- Southwest owns and operates its website at www.Southwest.com, its mobile applications,[10] and its API.[11] Southwest's API is not accessible by the general public and is only accessible by automated technology in specific pre-authorized scenarios.[12]

[6] D.I. 53, First Amended Complaint, at Ex. A.
[7] *See id.*
[8] *Thompson v. Chrysler Motors Corp.*, 755 F.2d 1162, 1165 (5th Cir. 1985).
[9] D.I. 53, First Amended Complaint.
[10] *Id.* at ¶ 2.
[11] *Id.* at ¶ 16. API is an interface used to programmatically access an application through a set of routines, protocols, and other tools for building software applications. The purpose of using an API is to access an application without using the standard user interface.
[12] *See* D.I. 41, Declaration of Michael Erdman at ¶ 12; D.I. 53, First Amended Complaint at ¶¶ 3, 32, 33.

- Southwest's fares and flight schedules are proprietary. Southwest maintains the exclusive online distribution rights to post fares and sell tickets through the Southwest Website.[13]

- Southwest does not allow online travel agencies ("OTAs") to sell Southwest flights without express written authorization. Southwest prohibits third-parties from accessing its flight information using "page scrape" technology.[14]

- Kiwi knowingly and intentionally targets the Southwest Website and API to harvest Southwest's fare and pricing information without Southwest's authorization.[15]

- Upon learning of Kiwi's conduct, Southwest sent cease-and-desist letters to Kiwi and filed this suit.[16]

- Kiwi operates an OTA business at kiwi.com that has engaged in repeated, unlawful activity on the Southwest Website, and ignored a series of cease-and-desist demands from Southwest.[17] Kiwi's unlawful conduct includes:

    - Page Scraping: Kiwi has knowingly violated the Website Terms through its unauthorized scraping of flight and pricing data from the Southwest Website;[18]

    - Unauthorized Access: Kiwi has violated federal and state law by continuing to access the Southwest Website without authorization from Southwest;[19]

- Since filing this lawsuit, Southwest has implemented security measures in an effort to stop Kiwi's activities, but Kiwi has continued to hack the Southwest Website, republish Southwest fares and flight schedules, and sell Southwest flights without permission;[20]

- Kiwi is accessing Southwest's computer systems located in Texas and in this District without authorization, bypassing Southwest's security systems intended to block automated traffic and bots from using the Southwest Website, and hacking the Southwest application program interface ("API") that is accessible only through the Southwest Website—all in violation of the Website Terms for use of the Southwest Website;[21]

- The Website Terms for use of the Southwest Website specifically prohibit, among other things, "use [of] any deep-link, page-scrape, robot, crawl, index, spider, macro programs, Internet agent, or other automatic device, program, algorithm or

[13] D.I. 53 at ¶ 32.
[14] *Id.* at ¶ 32.
[15] *Id.* at ¶ 40.
[16] *Id.* at ¶ 55.
[17] *Id.* at ¶ 5.
[18] *Id.* at ¶¶ 5-8.
[19] *Id.* at ¶ 5(a) and (e).
[20] *Id.* at ¶ 11.
[21] *Id.* at ¶ 16.

methodology which does the same things to use, access, copy, acquire information, ... search, generate searches, or monitor any portion of the [Southwest Website] or Company Information;"[22]

- Before February 24, 2021, Southwest application logs and automated bot protection product showed that Kiwi was using automated web-scraping script to access the "front end" of Southwest.com and scrape data ("Front-End Scraping");[23]

- On February 24, 2021, Southwest implemented a security measure that blocked Kiwi's Front-End Scraping. This was successful for a few weeks until Kiwi developed other hacks;[24]

- After the February 24th blocking measure, Kiwi began hacking Southwest's API with automated bots. After Kiwi determined how to bypass Southwest's automated bot detection, it attacked Southwest's API with automated scripts and continued to access, scrape, and republish Southwest data;[25]

- On the morning of April 5, 2021, Southwest implemented another measure to block Kiwi's API Hacking. Within eight hours of implementing this second blocking measure, Kiwi developed another hack to bypass Southwest's blocking technology; and[26]

- Kiwi continues to hack Southwest.com by changing the way it architects its automated scripts to access, scrape, and republish data from Southwest.com.[27]

III. ARGUMENT[28]

A. *Van Buren* does not allow Kiwi's hacking of Southwest's computers and API.

In considering the impact of *Van Buren* on Southwest's CFAA claim, the Court should consider the following. First, *Van Buren's* analysis is substantially limited to resolving a circuit

[22] *Id.* at ¶ 35.
[23] *Id.* at ¶ 76.
[24] *Id.* at ¶ 77.
[25] *Id.* at ¶ 79.
[26] *Id.* at ¶ 80.
[27] *Id.* at ¶ 81.
[28] As a threshold procedural matter, Kiwi.com, Inc.'s 12(c) motion is premature because Kiwi.com s.r.o. has not answered. FED. R. CIV. P. 12(C). The pleadings are not "closed" under Rule 12(c) until every defendant files an answer. *See e.g.*, *Watson v. County of Santa Clara,* No. C–06–04029, 2007 WL 2043852, at *1 (N.D.Cal. July 12, 2007) (denying Rule 12(c) motion as premature) (citing cases). In addition, Kiwi.com s.r.o.'s 12(b)(6) motion is untimely because it waived any such argument when it filed its previous 12(b)(6) motions to dismiss, which did not raise Southwest's CFAA claims. FED. R. CIV. P. 12(g)(2).

split over the meaning of the "*exceeds* authorization" clause of 18 U.S.C. § 1030(a)(2).[29] While Southwest's CFAA claim includes allegations that Kiwi exceeded authorized access by, among other things, using Southwest fare information for commercial purposes, Southwest also has alleged Kiwi accessed Southwest computers "without authorization" through its automated scraping and hacking. *Van Buren* does not meaningfully address this clause of the CFAA.

Second, *Van Buren* reaffirmed that the CFAA is "aimed" at protecting against "the typical consequences of hacking,"[30] and that the "'without authorization' clause protects computers themselves by targeting so-called outside hackers—those who 'acces[s] a computer without any permission at all.'"[31] It also confirmed that accessing data by circumventing a computer's security measures (*i.e.*, a "gates-down" environment) is actionable under the CFAA.[32]

Third, *Van Buren* expressly declined to consider whether the gates-down "inquiry turns only on technological (or 'code-based') limitations on access, or instead also looks to limits contained in contracts or policies."[33] Here, Kiwi does not dispute that Southwest's Website Terms impose contractual limitations on Kiwi's scraping and hacking, or that Southwest has repeatedly informed Kiwi that its automated access and API hacking are unauthorized.

Fourth, courts interpreting *Van Buren* already have recognized that issues, such as access and authorization, under the CFAA raise fact-intensive inquiries because it involves "questions regarding a person's authorized access and the scope of that authorization, as well as the specific

---

[29] *Van Buren*, 141 S. Ct. at 1649; *see United States v. Eddings*, 5:19-CR-00535, 2021 WL 2527966, at *5 (E.D. Pa. June 21, 2021) (distinguishing *Van Buren* from government theory under "without authorization" clause); *see also, Volpe v. Abacus Software Sys. Corp.*, CV2010108RMBKMW, 2021 WL 2451968, at *3 (D.N.J. June 16, 2021).
[30] *See Van Buren*, 141 S. Ct. at 1660.
[31] *See id.* at 1658 (quoting *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)).
[32] *Id.* at 1659.
[33] *See id.* at 1659 n. 8.

information he or she accessed and the location of that information"[34] that cannot be resolved on a Rule 12 motion.

B. Kiwi is accessing Southwest's gates-down computer(s) without authorization.

1. Kiwi is bypassing Southwest's electronic protections.

The Complaint contains detailed allegations showing that Kiwi is intentionally and electronically bypassing Southwest's security measures to access Southwest computer(s). For example, the Complaint makes the following unrefuted allegations:

- Kiwi has knowingly violated the Website Terms through its unauthorized scraping of flight and pricing data from the Southwest Website;[35]
- Since filing this lawsuit, Southwest has implemented self-help security measures in an effort to stop Kiwi's activities, but Kiwi has continued to hack the Southwest Website, republish Southwest fares and flight schedules, and sell Southwest flights without permission;
- Kiwi is bypassing Southwest's security systems intended to block automated traffic and bots from using the Southwest Website, and hacking Southwest's API;[36]
- On February 24, 2021, Southwest implemented a security measure that blocked Kiwi's Front-End Scraping. This was successful for a few weeks until Kiwi developed other hacks;[37]
- Soon after the February 24th blocking measure, Kiwi began hacking Southwest's API. After Kiwi determined how to bypass Southwest's automated bot detection, it attacked Southwest's API with automated scripts and continued to access, scrape, and republish Southwest data;[38]
- On the morning of April 5, 2021, Southwest implemented another measure to block Kiwi's API Hacking. Within eight hours of implementing this second blocking measure, Kiwi developed another hack to bypass Southwest's blocking technology.[39]

[34] *Leitner v. Morosvillo*, 21-CV-3075-SRB, 2021 WL 2669547, at *4 (W.D. Mo. June 29, 2021).
[35] D.I. 53 at ¶ 40.
[36] D.I. 53 at ¶ 11.
[37] *Id.* at ¶ 77.
[38] *Id.* at ¶ 79.
[39] *Id.* at ¶ 80.

- With each blocking measure Southwest implements, Kiwi continues to hack Southwest.com by changing the way it architects its automated scripts to access, scrape, and republish data from Southwest.com.[40]

These facts plainly support that Southwest's computers and API are "gates down" to Kiwi's automated scraping and hacking, and that Kiwi's access of Southwest computers is without authorization. *Van Buren* and other case law make clear that these digital trespasses are exactly the type of conduct the CFAA was intended to penalize. Based on these allegations alone, Kiwi's motion is without merit, and must be denied.

2. Kiwi is knowingly bypassing the Website Terms forbidding Kiwi's automated scraping, and has disregarded Southwest's repeated demands to cease its unauthorized access.

The Complaint also alleges that Kiwi's access is without authorization based on the Website Terms and Southwest's express cease and desist letters. The CFAA is an anti-trespass and anti-hacking statute.[41] "[A] defendant can run afoul of the CFAA when [it] has no permission to access a computer or when such permission has been revoked explicitly. Once permission has been revoked, technological gamesmanship [] will not excuse liability."[42] The Ninth Circuit's decision in *Facebook v. Power Ventures* is instructive. There, Power Ventures accessed Facebook through individual users' password-protected accounts, and refused to stop even after Facebook sent a cease and desist letter.[43] After Facebook instituted a technological block to prevent Power Ventures from accessing the Facebook website, Power Ventures circumvented the block.[44]

---

[40] *Id.* at ¶ 81.
[41] 28 U.S.C. § 1030; s*ee Facebook, Inc. v. Power Ventures, Inc*., 844 F.3d 1058, 1067 (9th Cir. 2016) (holding Power Ventures' intentional access of computers knowing that it was not authorized to do so was a violation of the CFAA).
[42] *See id.* at 1065.
[43] *See id.* at 1063.
[44] *See id.*

Facebook filed suit and the district court granted summary judgment to Facebook on its CFAA claim.[45]

On appeal, the Ninth Circuit found that the individual Facebook-users' grant of permission to Power Ventures to use each user's arguably "public" data "was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission" in the cease and desist letter.[46] The fact that Power Ventures deliberately disregarded the cease and desist letter, accessed Facebook's computers without authorization, and circumvented security barriers "demonstrated that [a website operator] had rescinded permission for [a scraper] to access [its] computers."[47] Thus, "Power [Ventures] accessed Facebook's computers 'without authorization' within the meaning of the CFAA and is liable under that statute."[48]

Decisions from courts in the Fifth Circuit are consistent with *Facebook.* For example, in *Southwest Airlines Co. v. Farechase, Inc.,*[49] the Northern District of Texas denied a motion to dismiss CFAA claims where: (a) the Website Terms prohibited the defendant's access of Southwest's computers; (b) the defendant *knew* that Southwest prohibited such conduct; and (c) Southwest directly informed the defendant that its conduct was prohibited.[50] The court noted that, regardless of whether the Website Terms created an enforceable contract, Southwest informed the defendant that its conduct was unauthorized and the defendant *knew* its conduct was not authorized by Southwest.

---

[45] *See id.* at 1064.
[46] *See id.* at 1068.
[47] *See id.*
[48] *See id.*
[49] *Sw. Airlines Co. v. Farechase, Inc*., 318 F. Supp. 2d 435 (N.D. Tex. 2004); *see e.g.*, *Sw. Airlines Co. v. Roundpipe, LLC*, 375 F. Supp. 3d 687, 689 (N.D. Tex. 2019).
[50] *Farechase*, 318 F. Supp. 2d at 439.

Similarly, the court in *DHI Group v. Kent* found that "a knowing violation of the terms and conditions of the website" by using "scraping crawling, or [] other automated means to download data from the website" was "sufficient to state a claim under [] the CFAA."[51] The court rejected the defendant's attempt to distinguish the alleged "browsewrap agreement" because the Plaintiff alleged a "*knowing* violation of terms and conditions contained in that browsewrap agreement."[52]

Southwest's CFAA claims against Kiwi are analogous to those in *Facebook, Farechase,* and *DHI.* The Complaint alleges that Kiwi violates Southwest's Website Terms when it bypasses Southwest's API and uses bots to gain access to Southwest's computers. And even after Southwest sent cease and desist letters, Kiwi: (a) "deliberately disregarded the cease and desist letter;" (b) "accessed [Southwest's] computers without authorization to do so;" and (c) circumvented Southwest's technological blocks (gates). For its part, Kiwi does not dispute that it is accessing and hacking Southwest's Website and API without Southwest's authorization, or that Southwest explicitly revoked any implicit authorization in its cease and desist letters to Kiwi.

Importantly, because *Van Buren* expressly declined to address whether contractual limits on authorized access support a CFAA claim, the Court should look to Fifth Circuit and other prevailing law on this point, including *Farechase*. Because Kiwi does not refute Southwest's allegations that: (a) the Terms and Conditions prohibit Kiwi's access of Southwest's computers; (b) Kiwi *knows* that Southwest prohibits such conduct; and (c) Southwest directly informed Kiwi that its conduct is prohibited, Southwest has stated a CFAA claim based on Kiwi's access of Southwest's computers and API without authorization. Kiwi's motion must be denied.[53]

---

[51] *DHI Group, Inc. v. Kent*, CV H-16-1670, 2017 WL 4837730, at *2, *9 (S.D. Tex. Oct. 26, 2017).
[52] *See id.* (emphasis in original).
[53] Although not necessary to deny Kiwi's motion, even if Kiwi's access to Southwest.com is not unauthorized, Southwest also has adequately pled that Kiwi has exceeded its authorization by,

Kiwi argues that by posting flights on Southwest.com for personal use (subject to the Website Terms), Southwest has opened the gates to any access, in any manner, by anyone. Kiwi manufactures an all-or-nothing gates theory where, by posting flights on Southwest.com for purchase by customers (gates up), Southwest has also left the gates up for Kiwi to use automated scraping and other hacks to access Southwest's computers and computer systems, even where Southwest has expressly forbidden such conduct and notified Kiwi that it is accessing Southwest's computer systems without authorization. Nothing in the CFAA or case law prevents a website owner from prohibiting certain methods of access to its computers, or from prohibiting specific persons from so accessing its computers. The Complaint alleges that Southwest—both contractually and by express written notice—has put the "gates down" for Kiwi's access to its website or API through automated hacking and scraping. Southwest has stated a valid CFAA claim under controlling law.

C. Southwest's CFAA claims are not subject to the heightened pleading standard.

Kiwi cites no authority for its argument that Southwest's CFAA claims are subject to the heightened pleading standard of Rule 9(c). In fact, the case law in the Fifth Circuit is clear that CFAA allegations need not meet the heightened standard.[54] Even if Southwest's CFAA claims

among other things, using automated bots and hacking Southwest's API, which is not generally open to the public.

[54] *EnviroGLAS Products, Inc. v. EnviroGLAS Products, LLC*, 705 F. Supp. 2d 560, 572 (N.D. Tex. 2010) ("Because the Computer Fraud and Abuse Act does not require a heightened pleading standard…the defendants' motion to dismiss this claim against them is denied.); *DHI Group, Inc. v. Kent*, CV H-16-1670, 2017 WL 1088352, at *12 (S.D. Tex. Mar. 3, 2017), report and recommendation adopted, CV H-16-1670, 2017 WL 1079184 (S.D. Tex. Mar. 22, 2017) ("Robins has cited no authority, and the court is aware of none, that the Fifth Circuit requires plaintiffs to meet the heightened pleading standard of Rule 9(b) for these computer access violations. While fraud is involved in [the CFAA], it is different from common law fraud that requires an actionable misrepresentation. Therefore, the court dismisses Robins' argument that Plaintiffs have failed to satisfy Rule 9(b).").

were subject to the heightened standard, Southwest has alleged specific facts showing the "who, what, where, when, and how" of the alleged "fraud."

IV. CONCLUSION

For the reasons discussed herein, Southwest has properly pled a CFAA claim. Southwest requests the court deny Kiwi.com, Inc's Rule 12(c) motion and Kiwi.com s.r.o.'s Rule 12(b)(6) motion to dismiss Southwest's CFAA claims. In the alternative, in the unlikely event the Court finds that Southwest's CFAA claims have not be adequately pled, Southwest requests the opportunity to replead.

Date: July 13, 2021

Respectfully submitted,

By: */s/ Michael C. Wilson*

Michael C. Wilson
Texas State Bar No. 21704590
mwilson@munckwilson.com
S. Wallace Dunwoody
Texas Bar. No. 24040838
wdunwoody@munckwilson.com
Amanda K. Greenspon
Florida Bar No. 1014584
agreenspon@munckwilson.com
Julie M. Christensen
Texas State Bar No. 24105601
jchristensen@munckwilson.com
MUNCK WILSON MANDALA, LLP
12770 Coit Road, Suite 600
Dallas, Texas 75251
Telephone: (972) 628-3600

COUNSEL FOR PLAINTIFF SOUTHWEST AIRLINES CO.

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was served on all counsel of record on July 13, 2021.

/s/ Michael C. Wilson
Michael C. Wilson

891064